

國立臺北科技大學 簽稿會核單

| | | | |
|-------|---|------|--------------|
| 案情摘要 | 檢送「臺灣學術網路 (TANet) 分散式阻斷服務 (DDoS) 通報應變作業指引」(如附件)，請查照辦理並轉知所屬相關單位。 | | |
| 主辦單位 | 計算機與網路中心 | 總收文號 | 1080015374 |
| 受會單位 | 會核意見及簽章 | | 收會時間 會畢時間 |
| 網路作業組 | <p>本校IP範圍140.124.0.0/16已於107年3月赴台大區網研議討論後，委請台大區網中心協助防禦Flow-based流量清洗作業，針對大流量DDoS攻擊協助清洗。惟Session-based因避免誤判爭議，由網路組資安設備協助清洗，進以達到低誤判並提高使系統高可用性。</p> <p>該日研議討論列席人員： 網路作業組(陳志豪) 台大區網中心(李美雯、游子興) 教育部資科司(林啟文)</p> <p>技術員 陳志豪 0516 1550</p> <p>網路組 王宜秀 0516 代理組長 1636</p> <p>計網中心 王永鐘 0517 主任 1601</p> | | |
| | | | |
| | | | |
| | | | |

裝

訂

線

便簽

日期：
單位：計算機與網路中心

- 一、文係教育部來函，檢送「臺灣學術網路分散式阻斷服務通報應變作業指引」，請本校查照並轉知所屬。
- 二、擬依來文旨揭，更新本中心資訊安全管理程序之法令法規遵循表，並EMAIL告知相關所屬人員，文陳閱後存查。

裝

訂

會辦單位： 網路作業組

| | |
|---|----------------------------------|
| 承辦單位 | 決行 |
| 技術員 林建成 0514 1540 系統組 黃慧娟 0514 代理組長 1640 技士 洪碧珍 0517 0739 計網中心 王永鐘 0517 主 任 1601 | 代為 決行 |
| 核稿單位 | 計網中心 王永鐘 0517 主 任 1601 |

線

檔 號：

保存年限：

教育部 函

機關地址：10051臺北市中山南路5號
傳 真：02-27377043
聯絡人：林啟文
電 話：02-7712-9091

受文者：國立臺北科技大學

發文日期：中華民國108年5月13日

發文字號：臺教資(四)字第1080063679號

速別：普通件

密等及解密條件或保密期限：

附件：臺灣學術網路 (TANet) 分散式阻斷服務 (DDoS) 通報應變作業指引(ATTCH2
A095N0000Q0000000_0063679A00_ATTCH2.pdf)

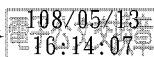
主旨：檢送「臺灣學術網路 (TANet) 分散式阻斷服務 (DDoS) 通報應變作業指引」(如附件)，請查照辦理並轉知所屬相關單位。

說明：

- 一、依據本部「臺灣學術網路管理小組第71次會議」會議紀錄辦理。
- 二、為提升臺灣學術網路 (TANet) 轄下各連線學校資安防護能量，降低學術網路之使用者受到分散式阻斷服務攻擊 (Distributed Denial of Service, DDoS) 之影響。本部於105年建置DDoS防護系統，供連線單位申請使用，並研擬本作業指引以資參考遵循。

正本：各直轄市及縣市政府教育局(處)、臺灣學術網路區域網路中心、各直轄市及縣市教育網路中心、各公私立大專校院(含大學系統)、各公私立高級中學、各公私立高級職業學校、各國立學校附設國民中小學、各國立國民小學、各私立國民中學、各私立國民小學

副本：國立中山大學、本部法制處



臺灣學術網路 (TANet)

分散式阻斷服務 (DDoS) 通報應變作業指引

一、目的

為有效提升臺灣學術網路 (TANet) 資安防護能量，降低學術網路之使用者受到分散式阻斷服務攻擊 (Distributed Denial of Service, DDoS) 之影響，教育部規劃「臺灣學術網路分散式阻斷服務通報應變作業指引」(以下稱本指引)，以緩解 DDoS 攻擊對各單位之影響，提昇臺灣學術網路之可用性與服務之品質。

二、適用對象

臺灣學術網路轄下各連線單位 (以下稱連線單位)。

三、適用範圍與限制

(一) 適用範圍

當發生 DDoS 攻擊時，連線單位可參考本指引，進行資安事件通報，並申請 DDoS 攻擊流量清洗服務或相關技術支援，以為攻擊事件之應變。

(二) 適用限制

本指引所提的流量清洗服務，僅限於經過臺灣學術網路各區域網路中心的 DDoS 攻擊流量；在 DDoS 攻擊流量清洗服務啟動後，除過濾異常網路流量外，可能會影響部份網路之連線。



四、DDoS 事件通報與應變作業程序

(一) 連線單位準備措施

1. 網域名稱系統 (Domain Name System, DNS) 服務與管理集中化

為避免 TANet 學術網路受 DDoS 攻擊而導致損害，連線單位應將單位內的 DNS 服務向上集中管理，並將單位內的 DNS 服務指向 TANet DNS，以保障 TANet 使用者之權益。

2. 網路拓樸圖清查與更新

為確保 DDoS 清洗服務達預期效果，連線單位應事先清查單位內線路並更新單位內網路拓樸圖，以為 DDoS 清洗服務之策略研判依據。網路拓譜圖應包含以下資訊，並事先提供本部及 DDoS 清洗服務單位備查：

- (1) 欲保護核心系統伺服器之 IP 位址；
- (2) 核心系統伺服器所提供的網路服務類別（如 80/TCP、53/UDP 等）；
- (3) 連線單位對外所有線路，包含臺灣學術網路及商用網路服務供應商。

(二) 分級措施

當連線單位遭受 DDoS 攻擊事件時，應依「教育體系 DDoS 攻擊清洗申請流程」（如附錄）進行相關作業；以下說明不同單位的分級措施。

1. 連線單位

- (1) 連線單位受到疑似 DDoS 攻擊時，應確認該攻擊事件是否影響單位內重要設施之運作，並通報上級連線單位（區、縣(市)網路中心）評估是否有 DDoS 攻擊流量清洗服務之必要性；倘若評估結果為必要，並由上級連線單位至「臺灣學術網路危機處理中心（TACERT）」提出申請。
- (2) 連線單位於 DDoS 清洗服務結束後，可參考《教育機構資安通報應變手冊》以及《國家資通安全通報應變作業綱要》，判定 DDoS 攻擊事件之事件等級，並依據資安事件等級，於時限內至 TACERT 的「教育機構資安通報平台」填寫《資安通報單》，以完成通報應變作業。「教育機構資安通報平台」網址為



<https://info.cert.tanet.edu.tw/>。

2. 區、縣（市）網路中心

- (1) 當區、縣(市)網路中心或轄下連線單位有必要申請 DDoS 清洗服務時，應由區、縣(市)網路中心至 TACERT 之「資安通報報表系統」項下的「DDoS 通報」提出申請。「資安通報報表系統」網址為 <https://portal.cert.tanet.edu.tw/index.html>。
- (2) 當區、縣（市）網路中心本身受攻擊而申請 DDoS 攻擊清洗服務結束後，亦應比照連線單位作為，判定 DDoS 攻擊事件之事件等級，並依據各資安事件等級之指引，於時限內至教育機構資安通報平台完成通報應變作業。
- (3) 區、縣（市）網路中心協助連線單位申請 DDoS 攻擊流量清洗服務應於服務結束後，由區、縣（市）網路人員登入 TACERT 之「教育機構資安通報平台」就連線單位所填寫的《資安通報單》內容進行審核，確認資安通報單內容的完整性，以及事件等級判斷的正確性。
- (4) 區、縣（市）網路中心的資安人員應掌握 DDoS 攻擊事件狀況，並提供必要之技術支援，協助連線單位進行事件之應變處理。

3. 學術資訊安全維運中心（Academic Security Operation Center, A-SOC）

- (1) 南區與北區的學術資訊安全維運中心（A-SOC）在偵測到大規模 DDoS 攻擊時，應分析 DDoS 攻擊流量以及攻擊手法，並發出資安警訊通知連線單位。
- (2) 南區與北區的 A-SOC 應依其服務範圍，於接獲 TACERT「DDoS 通報」申請或在教育部緊急通知時，提供 DDoS 攻擊流量清洗服務，並掌握重大 DDoS 攻擊事件細節，如攻擊事件之樣態、時間、來源與目標、攻擊軌跡以及緩解記錄等。必要時，A-SOC 可聯繫其他電信業者進行協同作業。

附錄：

教育體系DDoS攻擊清洗申請流程

2017.05.09

